UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,305	05/26/2000	STEFAN PHILIPP	PHD99-099	3907

7590 06/29/2004

Philips Electronic North American Corp.
580 White Plains Rd.
Tarrytown, NY 10591

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 06/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/555,305	PHILIPP, STEFAN	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-14 were pending for examination.

Claims 1, 6,8 and 14 are amended.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Yuliang Zheng, The SPEED Cipher in view of Sprunk.

As per (amended) claim 1, Zheng teaches the SPEED Cipher built on highly nonlinear Boolean functions, see Page 71, wherein, given a key K of l bits, SPEED scrambles a Plaintext M of w bits into a ciphertext of C of the same length see page 71.

Zheng teaches a block cipher method (i.e. The SPEED Cipher fi(x1, ki)) where a cryptographic sub-operation is performed on Plaintext M internally represented as 8 words (x0, x2 ,.....,x7), each with w/8 bits, and a cryptographic key K expanded by the key scheduling function into four sub-keys k1, k2, k3 and k4 each Ki consists of r/4 words or round keys indicating the number of round in each pass . Zheng's sub-operations operate employing a different sub-key, as well as a different bit-wise operation on the plaintext Xi, see Figures 1 and 2 pages 72-73, emphasis added by the Examiner to correspond to the amended feature.

Zheng's fails to teach a bit-wise operation depending on a control function ri based on random number.

However, Sprunk is directed to a secure microprocessor with reduced vulnerability to attack, see abstract.

In a preferred embodiment, Sprunk discloses a variable frequency source ("clock") which produces a clock signal with periodic clock pulses. That is, the variable selection of the microprocessor clock is affected using a random "modulation" circuit that randomly varies each pulse of the clock signal to render the timing of successive pulses unpredictable and used to clock a crypto processor for the encryption or decryption of data entered, see col. 3, line 66 through col. 4, line 13.

It would have been obvious to one of ordinary skill in the art to adapt the crypto processor implementing the SPEED Cipher of Zheng to that of Sprunck to prevent pirates to modify the operations of the crypto processor because the ability of pirates to observe such clock signals is critical in mounting a successful attack to the system security, see col. 1, lines 38-49.

As per claim 2, Zheng teaches one or more XOR (exclusive Or) combinations formed during the cryptographic sub-operations, see Page 74, table 2.

As per claim 3, Zheng teaches that data contain cryptographic keys (i.e. sub-keys) and /or operand (i.e. Xi plaintext), see Fig. 1 and Table 2.

As per claims 4-5, 7 and (amended) claim 6 , Zheng's SPEED Cipher uses the intermediate results from each round (sub-operation) as an operand for the subsequent Cryptographic sub-operations, see Fig.4, and that output of one round is fed as an input to the succeeding round of operations, see Fig.2.

Zheng further teaches that during bit-wise operation seven 8-bit operand (xi) are invereted, see page 74, table 2 (*for the claimed even bit values, the odd bit values or all bit values recited in claim 6).*

Zheng further teaches that the bit values of a data bit word of plaintext or subkeys are inverted by means of an XOR operation, see, page 74, Table 2, For example in P1 F1(x6, x5,.....x0)=x6x3 XOR x5x1XOR.....XORx0 where XiXj is bit-wise AND and Xi XOR Xj is the Bit-wise XOR of the two words and that in a pass Pi in SPEED the content in registers are updated accordingly, see page 76., see also the "Round transform" on page 78.

Claims 8(amended), 9-13, and 14 (amended) are apparatus claims corresponding to method claims 1-7, Claims 8-14 are rejected for the same reasons stated in the statement of rejection of claims 1-7 above.

Response to Amendment

Applicant's arguments filed on 4/5/2004 regarding the rejection of the claims 1-14 under 35 U.S.C. 103() have been fully considered but they are not persuasive.

As per Applicant arguments relating to the rejection of claims 1 and 8, the applicant argues that "the modulated clock signal described in Sprunk causes the microprocessor to perform operations (or not) depending on the unpredictable stream of clock pulses" and that " the modulated clock signal only controls when the operations are performed and does not control how the operations are performed", page 5 of REMARKS third paragraph.

The Examiner responds that the specific of claimed invention as how (not when) the operations are performed is not claimed and that the claimed invention of bit-wise operations

depending on "a control signal ri which is based on a random number" is broadly interpreted as how and when the operations are performed. Furthermore, while the examiner reads the claims in light of specification, the examiner declines to read the limitations from the specification into the claim.

As per Applicant's arguments relating to Sprunk reference, the Applicant argues that Sprunk fails to teach or suggest that at least one cryptographic sub-operation is performed using data and/or a result that is bit-wise complement or not", same page and paragraph.

The Examiner responds that this feature is taught by the primary reference of Zheng ("the SPEED Cipher"). The Sprunk reference in a 103 type rejection is used for its "control function.... based on random number".

Action is Final

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner

November 24, 203

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100